

Properties of cuspidal divisor class numbers of non-split Cartan modular curves

Pierfrancesco Carlucci

Dipartimento di Matematica

Università degli studi di Roma Tor Vergata

Via della Ricerca Scientifica 1, 00133, Rome, Italy

E-mail: pieffecar@libero.it

30 May, 2016

Abstract

Let $\mathfrak{C}_{ns}^+(p)$ be the Cuspidal Divisor Class Group of the modular curves $X_{ns}^+(p)$ associated to the normalizer of a non-split Cartan subgroup of level p . I study the p -primary part of $\mathfrak{C}_{ns}^+(p)$ and estimate the order of growth of $|\mathfrak{C}_{ns}^+(p)|$.

1 Introduction

Let p be a prime and let $X_{ns}^+(p^k)$ be the modular curve associated to the normalizer of a non-split Cartan subgroup of level p^k . In [2] we describe the Cuspidal Divisor Class Group $\mathfrak{C}_{ns}^+(p^k)$ on $X_{ns}^+(p^k)$ as a module over the group ring $\mathbb{Z}[(\mathbb{Z}/p^k\mathbb{Z})^*/\{\pm 1\}]$. Let w be a generator of $H = (\mathbb{Z}/p\mathbb{Z})^*/\{\pm 1\}$ and let ω be a generator of the character group $\hat{\mathbb{F}}_{p^2}^*$. Define $d = \frac{12}{\gcd(12, p+1)}$, the group ring $R = \mathbb{Z}[H]$, the ideals:

$$R_0 := \left\{ \sum b_j w^j \in R \text{ such that } \deg \left(\sum b_j w^j \right) = \sum b_j = 0 \right\},$$

$$R_d := \left\{ \sum b_j w^j \in R \text{ such that } d \text{ divides } \deg \left(\sum b_j w^j \right) = \sum b_j \right\},$$

2010 *Mathematics Subject Classification*: Primary 11B68; Secondary 11M41, 13C20.

Key words and phrases: Cuspidal Divisor Class Number, Non-Split Cartan Curves, Generalized Bernoulli Numbers, L-functions, Regular and Irregular Primes.

the Stickelberger element:

$$\theta = \frac{p}{2} \sum_{i=0}^{\frac{p-3}{2}} \sum_{\substack{x \in \mathbb{F}_2^*/\{\pm 1\} \\ \pm x^{p+1} = w^i}} B_2 \left(\left\langle \frac{\frac{1}{2}(\text{Tr}(x))}{p} \right\rangle \right) w^{-i} \in \mathbb{Q}[H]$$

and the generalized Bernoulli number:

$$B_{2,\chi} = \sum_{x \in \mathbb{F}_2^*/\{\pm 1\}} B_2 \left(\left\langle \frac{\frac{1}{2}\text{Tr}(x)}{p} \right\rangle \right) \chi(x).$$

Specializing [2, Theorem 7.1] and [2, Theorem 7.4] to the case $k = 1$ we obtain:

Theorem 1.1. *The Cuspidal Divisor Class Group on $X_{ns}^+(p)$ is a module over R and we have the following isomorphism:*

$$\mathfrak{C}_{ns}^+(p) \cong R_0/R_d\theta.$$

Moreover we have:

$$|\mathfrak{C}_{ns}^+(p)| = \frac{24}{(p-1)\gcd(12, p+1)} \prod_{j=1}^{\frac{p-3}{2}} \frac{p}{2} B_{2,\omega^{(2p+2)j}}.$$

From the previous theorem we deduce two results both having a counterpart in cyclotomic field theory.

Theorem 2.1 *We have:*

$$\ln |\mathfrak{C}_{ns}^+(p)| = p \ln p + \Theta(p).$$

The paper ends up with a modular analogue of Mazur-Wiles [9, pag. 300], Herbrand [9, pag. 101] and Ribet [9, pag. 342] theorems for cyclotomic fields. We have a similar piece by piece description of the p -Sylow part \mathcal{C}_p of $\mathfrak{C}_{ns}^+(p)$. Let A be the p -Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_p)$. A corollary of Mazur-Wiles theorem states that:

$$|A(\omega^i)| = p\text{-part of } B_{1,\omega^{-i}} \text{ (} i \not\equiv 1 \pmod{p-1}, i \text{ odd)}.$$

A reformulation of Kubert and Lang Theorems 4.2 and 4.3 of [6, Chapter 5], enables us to deduce that, as in the cyclotomic field theory, $|\mathcal{C}_p(\omega^{2j})|$ are strictly related to the p -parts of certain generalized Bernoulli numbers $B_{2,\omega^{4j}}$. Usually we expect that $\mathcal{C}_p \cong (\mathbb{Z}/p\mathbb{Z})^{\lfloor \frac{p}{4} \rfloor - 1}$ and exceptions occur only

when p is an irregular prime. More precisely:

Theorem 3.2 $\text{ord}_p(|\mathfrak{C}_{ns}^+(p)|) = [\frac{p}{4}] - 1$ if and only if p is a regular prime or $p \equiv 1 \pmod{4}$ is irregular and p does not divide the numerator of any Bernoulli number b_{4j+2} for $j \leq \frac{p-5}{4}$.

If $\text{ord}_p(|\mathfrak{C}_{ns}^+(p)|) = [\frac{p}{4}] - 1$ we have $\mathcal{C}_p \cong (\mathbb{Z}/p\mathbb{Z})^{[\frac{p}{4}]-1}$.

If $p \equiv 1 \pmod{4}$ and $\text{ord}_p(|\mathfrak{C}_{ns}^+(p)|) > [\frac{p}{4}] - 1$ then $\mathfrak{C}_{ns}^+(p)$ contains an element of order p^2 .

If $p \equiv 3 \pmod{4}$ and $\text{ord}_p(|\mathfrak{C}_{ns}^+(p)|) > [\frac{p}{4}] - 1$ then $\mathfrak{C}_{ns}^+(p)$ contains an element of order p^2 if and only if p divides b_{4j+2} for some $j \leq \frac{p-7}{4}$.

If $p \equiv 3 \pmod{4}$ then $\text{ord}_p(|\mathfrak{C}_{ns}^+(p)|) \geq [\frac{p}{4}] - 1 + \text{irr}(p)$ where $\text{irr}(p)$ is the index of irregularity of p .

2 Order of growth of Cuspidal Divisor Class Groups

We study the order of growth of $|\mathfrak{C}_{ns}^+(p)|$:

Theorem 2.1. If $p \equiv 1 \pmod{4}$:

$$|\mathfrak{C}_{ns}^+(p)| = \mathcal{O} \left(\left(\frac{p}{2\sqrt{6}} \right)^{p-4} \right).$$

If $p \equiv 3 \pmod{4}$:

$$|\mathfrak{C}_{ns}^+(p)| = \mathcal{O} \left(\left(\frac{p}{2\sqrt[4]{90}} \right)^{p-4} \right).$$

Furthermore for every p we have:

$$|\mathfrak{C}_{ns}^+(p)| = \Omega \left(\left(\frac{p}{2\pi} \right)^{p-4} \right)$$

so

$$\ln |\mathfrak{C}_{ns}^+(p)| - p \ln p = \Theta(p).$$

Proof. Let $T : \mathbb{F}_{p^2} \rightarrow \mathbb{F}_p$ a surjective \mathbb{F}_p -linear map. Let χ be a multiplicative character on $\mathbb{F}_{p^2}^*$. Following [6, Paragraph 1.5] and [5] we define for $s \in \mathbb{C}$ the generalized L -series:

$$L(s, \chi, T) = p^{-s-1} \sum_{\alpha \in \mathbb{F}_{p^2}} \chi(\alpha) \zeta \left(s, \left\langle \frac{T(\alpha)}{p} \right\rangle \right)$$

where $\zeta(s, u)$ is the Hurwitz zeta function which is defined for a real number $0 < u \leq 1$ by:

$$\zeta(s, u) = \sum_{n=0}^{\infty} \frac{1}{(n+u)^s}.$$

By a classical result of Hurwitz [9, Theorem 4.2] we have:

$$\zeta(1-m, u) = -\frac{1}{m} B_m(u)$$

so if χ is an even character and $T(\alpha) := \frac{1}{2} \text{Tr}(\alpha) \bmod p$, we have:

$$B_{2,\chi} = -L(-1, \chi, T).$$

Consider the following relation (cfr. [6, Theorem 5.2, Chapter 1]):

$$L(s, \chi, T) = \frac{1}{2\pi i} \left(\frac{2\pi}{p} \right)^s \Gamma(1-s) \tau(\chi, T) [e^{\frac{\pi i s}{2}} - \chi(-1) e^{-\frac{\pi i s}{2}}] L(1-s, \chi|_{\mathbb{F}_p})$$

where $L(1-s, \chi|_{\mathbb{F}_p})$ is an ordinary L -function and

$$\tau(\chi, T) = \sum_{\alpha \in \mathbb{F}_{p^2}} \chi(\alpha) e^{\frac{2\pi i T(\alpha)}{p}}$$

is a Gauss sum on \mathbb{F}_{p^2} . From [4, Proposition 11.5] we have $|\tau(\chi, T)| = p$ so by virtue of Theorem 1.1 we deduce:

$$|\mathfrak{C}_{ns}^+(p)| = \Theta \left(\left(\frac{p}{2\pi} \right)^{p-4} \prod_{j=1}^{\frac{p-3}{2}} |L(2, (\omega^{(2p+2)j})|_{\mathbb{F}_p})| \right).$$

If $p \equiv 1 \bmod 4$ let B the subgroup of squares of even characters mod p .

In this case we have:

$$\begin{aligned} \left| \prod_{j=1}^{\frac{p-3}{2}} L(2, (\omega^{(2p+2)j})|_{\mathbb{F}_p}) \right| &= \left| \prod_{\chi \neq 1 \text{ even}} L(2, \chi^2) \right| = \\ &= \left| \zeta(2) \prod_{\chi \neq 1, \chi \in B} L(2, \chi)^2 \right| \leq \zeta(2)^{\frac{p-3}{2}}, \\ |\mathfrak{C}_{ns}^+(p)| &= \mathcal{O} \left(\left(\frac{p}{2\sqrt{6}} \right)^{p-4} \right). \end{aligned}$$

If $p \equiv 3 \bmod 4$ we can obtain a more accurate estimation. In this case we have:

$$\prod_{j=1}^{\frac{p-3}{2}} L(2, (\omega^{(2p+2)j})|_{\mathbb{F}_p}) = \prod_{\chi \neq 1 \text{ even}} L(2, \chi)$$

and by the arithmetic-geometric mean inequality:

$$\left| \prod_{\chi \neq 1 \text{ even}} L(2, \chi)^2 \right|^{\frac{2}{p-3}} \leq \frac{2}{p-3} \sum_{\chi \neq 1 \text{ even}} |L(2, \chi)|^2.$$

For $t \geq \frac{p+1}{2}$ let $S(t, \chi) = \sum_{\frac{p+1}{2} \leq n < t} \chi(n)$, then:

$$L(2, \chi) = \sum_{n=1}^{\frac{p-1}{2}} \frac{\chi(n)}{n^2} + 2 \int_{\frac{p+1}{2}}^{\infty} \frac{S(t, \chi)}{t^3} dt.$$

From the Polya-Vinogradov inequality [4, Theorem 12.5] for every $\chi \neq 1$ we have $|S(t, \chi)| \leq 6\sqrt{p} \ln p$ and consequently:

$$|L(2, \chi)| \leq \left| \sum_{n=1}^{\frac{p-1}{2}} \frac{\chi(n)}{n^2} \right| + \frac{24\sqrt{p} \ln p}{(p+1)^2}.$$

By the triangle inequality we obtain:

$$\begin{aligned} \left(\sum_{\chi \neq 1 \text{ even}} |L(2, \chi)|^2 \right)^{\frac{1}{2}} &\leq \left(\sum_{\chi \neq 1 \text{ even}} \left| \sum_{n=1}^{\frac{p-1}{2}} \frac{\chi(n)}{n^2} \right|^2 \right)^{\frac{1}{2}} + \left(\sum_{\chi \neq 1 \text{ even}} \left(\frac{24\sqrt{p} \ln p}{(p+1)^2} \right)^2 \right)^{\frac{1}{2}} \\ &\leq \left(\sum_{\chi \text{ even}} \left| \sum_{n=1}^{\frac{p-1}{2}} \frac{\chi(n)}{n^2} \right|^2 \right)^{\frac{1}{2}} + \frac{24\sqrt{p} \ln p}{(p+1)^2} \sqrt{\frac{p-3}{2}} \\ &\leq \pi^2 \sqrt{\frac{p-1}{180}} + \frac{24\sqrt{p} \ln p}{(p+1)^2} \sqrt{\frac{p-3}{2}} \end{aligned}$$

because:

$$\sum_{\chi \text{ even}} \left| \sum_{n=1}^{\frac{p-1}{2}} \frac{\chi(n)}{n^2} \right|^2 = \sum_{\chi \text{ even}} \sum_{n=1}^{\frac{p-1}{2}} \sum_{m=1}^{\frac{p-1}{2}} \frac{\chi(n) \bar{\chi}(m)}{n^2 m^2} = \frac{p-1}{2} \sum_{n=1}^{\frac{p-1}{2}} \frac{1}{n^4} \leq \frac{p-1}{2} \zeta(4)$$

and $\sum_{\chi \text{ even}} \chi(n) \bar{\chi}(m) = 0$ except when $n \equiv \pm m \pmod{p}$. Hence:

$$\left| \prod_{\chi \neq 1 \text{ even}} L(2, \chi)^2 \right|^{\frac{2}{p-3}} \leq \frac{2}{p-3} \left(\pi^2 \sqrt{\frac{p-1}{180}} + \frac{24\sqrt{p} \ln p}{(p+1)^2} \sqrt{\frac{p-3}{2}} \right)^2,$$

$$\frac{2}{p-3} \left(\pi^2 \sqrt{\frac{p-1}{180}} + \frac{24\sqrt{p} \ln p}{(p+1)^2} \sqrt{\frac{p-3}{2}} \right)^2 = \frac{\pi^4}{90} + \mathcal{O}\left(\frac{1}{p}\right),$$

$$\left| \prod_{\chi \neq 1 \text{ even}} L(2, \chi) \right| = \mathcal{O}\left(\left(\frac{\pi}{\sqrt[4]{90}}\right)^p\right),$$

$$|\mathfrak{C}_{ns}^+(p)| = \mathcal{O} \left(\left(\frac{p}{2\sqrt[4]{90}} \right)^{p-4} \right).$$

Let Λ be the von Mangoldt function:

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some prime } p \text{ and integer } k \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

From the classical relation:

$$\ln L(s, \chi) = \sum_{n=2}^{\infty} \frac{\Lambda(n)}{\ln n} \chi(n) n^{-s}$$

we have that if $p \equiv 1 \pmod{4}$:

$$\begin{aligned} \prod_{\chi \in B} L(2, \chi) &= \exp \left(\sum_{\chi \in B} \sum_{n=2}^{\infty} \frac{\Lambda(n)}{n^2 \ln n} \chi(n) \right) = \\ &= \exp \left(\frac{p-1}{4} \sum_{\substack{n=2 \\ n^4 \equiv 1 \pmod{p}}}^{\infty} \frac{\Lambda(n)}{n^2 \ln n} \right) \geq 1 \end{aligned}$$

and analogously if $p \equiv 3 \pmod{4}$ we have: $\prod_{\chi \text{ even}} L(2, \chi) \geq 1$.

Alternatively, we could notice that if X is a group of Dirichlet characters and K is the associated field with ring of integers \mathcal{O}_K , from [9, Theorem 4.3] we have:

$$\prod_{\chi \in X} L(2, \chi) = \zeta_K(2) = 1 + \sum_{I \subsetneq \mathcal{O}_K} \frac{1}{[\mathcal{O}_K : I]^2} > 1.$$

So we can easily deduce:

$$|\mathfrak{C}_{ns}^+(p)| = \Omega \left(\left(\frac{p}{2\pi} \right)^{p-4} \right)$$

and

$$\ln |\mathfrak{C}_{ns}^+(p)| - p \ln p = \Theta(p).$$

□

3 Eigencomponents at prime level

Following [7], in order to study the p -primary part \mathcal{C}_p of $\mathfrak{C}_{ns}^+(p)$ it is convenient to define:

$$R_p := \mathbb{Z}_p[H] \text{ with } H = (\mathbb{Z}/p\mathbb{Z})^*/(\pm 1),$$

$$R_{p,0} := \{x \in R_p \text{ of degree } 0\},$$

where the degree of $x = \sum_{h \in H} x_h h$ is defined by $\deg x = \sum_{h \in H} x_h$. Of course we have $\mathcal{C}_p \cong R_{p,0}/R_p \theta$ because when $p \geq 5$, the Stickelberger element θ belongs to $\frac{1}{12}\mathbb{Z}[H]$ and 12 is invertible in \mathbb{Z}_p . We have the following decomposition:

$$\mathbb{Z}_p \otimes \mathcal{C}_p = \bigoplus_{\chi} \mathcal{C}_p(\chi),$$

where χ ranges over the non trivial characters:

$$\chi : (\mathbb{Z}/p\mathbb{Z})^*/(\pm 1) \rightarrow \mathbb{Z}_p^*$$

and $a \in \mathcal{C}_p(\chi)$ if and only if $a \cdot b = \chi(b) \cdot a$ for every $b \in \mathbb{Z}_p \otimes \mathcal{C}_p$.

Let w be a generator of $H = (\mathbb{Z}/p\mathbb{Z})^*/\{\pm 1\}$. Notice that:

$$\chi(\theta) = \frac{p}{2} \sum_{i=0}^{\frac{p-3}{2}} \sum_{\substack{x \in (\mathbb{F}_{p^2}^*/\{\pm 1\}) \\ \pm x^{p+1} = w^i}} B_2 \left(\left\langle \frac{\frac{1}{2}(\text{Tr}(x))}{p} \right\rangle \right) \chi^{-1}(w^i) := S_{\chi^{-1}},$$

so θ operates on $\mathcal{C}_p(\chi)$ as multiplication by $S_{\chi^{-1}}$ and consequently:

$$\mathcal{C}_p(\chi) = \mathbb{Z}_p / S_{\chi^{-1}} \mathbb{Z}_p.$$

We define the Teichmüller character

$$\omega : \mathbb{F}_p^* \rightarrow \mathbb{Z}_p^*$$

to be the character such that:

$$\omega(a) = a \bmod p.$$

Then we consider $\phi = \omega^2$ and view it as a character on H .

Proposition 3.1. *Define:*

$$B'_{2,\phi^j} := B_{2,\omega^{4j}} = p \sum_{a=1}^{p-1} \phi^{2j}(a) B_2 \left(\frac{a}{p} \right).$$

If $p \equiv 1 \bmod 4$ and $1 \leq j \leq \frac{p-5}{4}$: $\text{ord}_p S_{\phi^j} = 1 + \text{ord}_p B'_{2,\phi^j} \geq 1$.

If $p \equiv 1 \bmod 4$ and $j = \frac{p-1}{4}$: $\text{ord}_p S_{\phi^{\frac{p-1}{4}}} = 0$.

If $p \equiv 1 \bmod 4$ and $\frac{p+3}{4} \leq j \leq \frac{p-3}{2}$: $\text{ord}_p S_{\phi^j} = \text{ord}_p B'_{2,\phi^j} \geq 0$.

If $p \equiv 3 \bmod 4$ and $1 \leq j \leq \frac{p-7}{4}$: $\text{ord}_p S_{\phi^j} = 1 + \text{ord}_p B'_{2,\phi^j} \geq 1$.

If $p \equiv 3 \bmod 4$ and $j = \frac{p-3}{4}$: $\text{ord}_p S_{\phi^{\frac{p-3}{4}}} = 1 + \text{ord}_p B'_{2,\phi^{\frac{p-3}{4}}} = 0$.

If $p \equiv 3 \bmod 4$ and $\frac{p+1}{4} \leq j \leq \frac{p-3}{2}$: $\text{ord}_p S_{\phi^j} = \text{ord}_p B'_{2,\phi^j} \geq 0$.

Proof. Corollary of Theorems 4.2 and 4.3 of [6, Chapter 5]. \square

It is immediate to deduce that $\text{ord}_p(|\mathfrak{C}_{ns}^+(p)|) \geq [\frac{p}{4}] - 1$. From [9, Theorem 5.16] we recall that a prime is regular (i.e. does not divide h_p^- , the relative class number of the cyclotomic fields $\mathbb{Q}(\zeta_p)$), if and only if p does not divide the numerator of any of the Bernoulli numbers b_n for $n = 2, 4, 6, \dots, p-3$. We propose an analogue for the modular case of Mazur-Wiles [9, Chapter 13] and Herbrand-Ribet theorems [9, Chapters 6 and 15] for cyclotomic fields. Usually we expect $\mathcal{C}_p \cong (\mathbb{Z}/p\mathbb{Z})^{[\frac{p}{4}]-1}$ and exceptions occur only when p is an irregular prime.

Theorem 3.2. *$\text{ord}_p(|\mathfrak{C}_{ns}^+(p)|) = [\frac{p}{4}] - 1$ if and only if p is a regular prime or $p \equiv 1 \pmod{4}$ is irregular and p does not divide the numerator of any Bernoulli number b_{4j+2} for $j \leq \frac{p-5}{4}$.*

If $\text{ord}_p(|\mathfrak{C}_{ns}^+(p)|) = [\frac{p}{4}] - 1$ we have $\mathcal{C}_p \cong (\mathbb{Z}/p\mathbb{Z})^{[\frac{p}{4}]-1}$.

If $p \equiv 1 \pmod{4}$ and $\text{ord}_p(|\mathfrak{C}_{ns}^+(p)|) > [\frac{p}{4}] - 1$ then $\mathfrak{C}_{ns}^+(p)$ contains an element of order p^2 .

If $p \equiv 3 \pmod{4}$ and $\text{ord}_p(|\mathfrak{C}_{ns}^+(p)|) > [\frac{p}{4}] - 1$ then $\mathfrak{C}_{ns}^+(p)$ contains an element of order p^2 if and only if p divides b_{4j+2} for some $j \leq \frac{p-7}{4}$.

If $p \equiv 3 \pmod{4}$ then $\text{ord}_p(|\mathfrak{C}_{ns}^+(p)|) \geq [\frac{p}{4}] - 1 + \text{irr}(p)$ where $\text{irr}(p)$ is the index of irregularity of p .

Proof. Let $1 \leq a \leq p-1$. From Proposition 3.1, we need to investigate when p divides B'_{2,ϕ^j} . We will provide an alternative proof of Von Staudt type congruences [6, p.125]:

$$\frac{1}{n} B_{n,\omega^{k-n}} = \frac{1}{k} B_k \pmod{p}$$

in the case $k = 2$. For the general case see [8, Chapter 2, Theorem 2.5]. We have:

$$B'_{2,\phi^j} = \frac{p}{6} \sum_{i=1}^{p-1} \omega^{4j}(a) - \sum_{i=1}^{p-1} a \omega^{4j}(a) + \frac{1}{p} \sum_{i=1}^{p-1} a^2 \omega^{4j}(a).$$

But $\sum_{i=1}^{p-1} a \omega^{4j}(a) \equiv \sum_{i=1}^{p-1} a^{4j+1} \equiv 0 \pmod{p}$, so $pB'_{2,\phi^j} \equiv \sum_{i=1}^{p-1} a^2 \omega^{4j}(a) \pmod{p^2}$.

If $p \equiv 3 \pmod{4}$ and $j = \frac{p-3}{4}$ we have $\sum_{i=1}^{p-1} a^2 \omega^{p-3}(a) \equiv -1 \pmod{p}$ and $\text{ord}_p B'_{2,\phi^{\frac{p-3}{4}}} = -1$. Apart from this exception we have that $p \mid \sum_{i=1}^{p-1} a^2 \omega^{4j}(a)$ and $\text{ord}_p B'_{2,\phi^j} \geq 0$.

Let $\omega_1(a) \in \mathbb{Z}$ with $1 \leq \omega_1(a) \leq p-1$ chosen so that we have $\omega(a) = a + \omega_1(a)p \pmod{p^2}$. Since $\omega(a)^p = \omega(a)$ we deduce $\omega_1(a) \equiv \frac{a^p - a}{p} \pmod{p}$. Ergo:

$$pB'_{2,\phi^j} \equiv \sum_{i=1}^{p-1} a^2 (a + \omega_1(a)p)^{4j} \pmod{p^2}$$

$$\begin{aligned}
&\equiv \sum_{i=1}^{p-1} a^2(a^{4j} + 4ja^{4j-1}p\omega_1(a)) \bmod p^2 \\
&\equiv \sum_{i=1}^{p-1} a^2(a^{4j} + 4ja^{4j-1}(a^p - a)) \bmod p^2 \\
&\equiv (1 - 4j) \sum_{i=1}^{p-1} a^{4j+2} + 4j \sum_{i=1}^{p-1} a^{4j+1+p} \bmod p^2.
\end{aligned}$$

Let $B_n(x)$ the n -th Bernoulli polynomial. From Faulhaber's formula (cf. [1, Theorem 1.5] and [3, Proposition 9.2.12]) we have:

$$pB'_{2,\phi^j} \equiv (1 - 4j) \frac{B_{4j+3}(p) - B_{4j+3}(0)}{4j+3} + 4j \frac{B_{4j+2+p}(p) - B_{4j+2+p}(0)}{4j+2+p} \bmod p^2.$$

But $B_n(x) = \sum_{h=0}^n \binom{n}{h} b_{n-h} x^h$ so we obtain:

$$pB'_{2,\phi^j} \equiv p(1 - 4j)b_{4j+2} + 4pj b_{4j+1+p} \bmod p^2,$$

$$B'_{2,\phi^j} \equiv (1 - 4j)b_{4j+2} + 4j b_{4j+1+p} \bmod p.$$

Notice that for $1 \leq j \leq \frac{p-3}{2}$, $p-1$ does divide neither $4j+2$ nor $4j+1+p$ (we have already excluded the case $p \equiv 3 \bmod 4$ and $j = \frac{p-3}{4}$). We may apply Kummer's congruence [1, Theorem 3.2]:

$$b_{4j+1+p} \equiv \frac{4j+1+p}{4j+2} b_{4j+2} \bmod p.$$

So we have:

$$B'_{2,\phi^j} \equiv b_{4j+2} \left(1 - 4j + 4j \frac{4j+1+p}{4j+2} \right) \bmod p.$$

But $(1 - 4j + 4j \frac{4j+1+p}{4j+2}) \equiv \frac{1}{2j+1} \bmod p$, so p divides B'_{2,ϕ^j} if and only if p divides b_{4j+2} .

If $p \equiv 1 \bmod 4$ and $\frac{p+3}{4} \leq j \leq \frac{p-3}{2}$ we have that p divides b_{4j+2} , if and only if p divides $b_{4j+3-p} = b_{4(j-\frac{p-1}{4})+2}$ so $\text{ord}_p(|\mathfrak{C}_{ns}^+(p)|) = [\frac{p}{4}] - 1$, if and only if p is regular or p is irregular, but p does not divide the numerator of any b_{4j+2} for $j \leq \frac{p-5}{4}$.

If $p \equiv 3 \bmod 4$ and $\frac{p+1}{4} \leq j \leq \frac{p-3}{2}$, we have that p divides b_{4j+2} if and only if p divides $b_{4j+3-p} = b_{4(j-\frac{p-3}{4})}$. So in this case $\text{ord}_p(|\mathfrak{C}_{ns}^+(p)|) > [\frac{p}{4}] - 1$, if and only if p is irregular.

The first claim is proved. The other assertions follow from Proposition 3.1.

□

The table below is an excerpt of [2, Table 8.1]:

p	$ \mathfrak{C}_{ns}^+(p) $
23	$23^4 \cdot 37181$
37	$3^4 \cdot 7^2 \cdot 19^3 \cdot 37^8 \cdot 577^2$
43	$2^2 \cdot 19 \cdot 29 \cdot 43^9 \cdot 463 \cdot 1051 \cdot 416532733$
59	$59^{14} \cdot 9988553613691393812358794271$
67	$67^{16} \cdot 193 \cdot 661^2 \cdot 2861 \cdot 8009 \cdot 11287 \cdot 9383200455691459$
73	$2^2 \cdot 3^4 \cdot 11^2 \cdot 37 \cdot 73^{17} \cdot 79^2 \cdot 241^2 \cdot 3341773^2 \cdot 11596933^2$
89	$2^2 \cdot 3 \cdot 5 \cdot 11^2 \cdot 13^2 \cdot 89^{21} \cdot 4027^2 \cdot 262504573^2 \cdot 15354699728897^2$
101	$5^4 \cdot 17 \cdot 101^{24} \cdot 52951^2 \cdot 54371^2 \cdot 58884077243434864347851^2$

The first four irregular primes are 37, 59, 67 and 101. Since $37|b_{32}$, $59|b_{44}$, $67|b_{58}$ and $101|b_{68}$ according to Theorem 3.2 we immediately deduce that:

$$\mathcal{C}_{37} \cong (\mathbb{Z}/37\mathbb{Z})^8, \mathcal{C}_{101} \cong (\mathbb{Z}/101\mathbb{Z})^{24}$$

and $\text{ord}_p(|\mathfrak{C}_{ns}^+(p)|) > [\frac{p}{4}] - 1$ for $p = 59, 67$. Moreover, knowing from explicit calculation that $\text{ord}_{59}(|\mathfrak{C}_{ns}^+(59)|) = 14$, $\text{ord}_{67}(|\mathfrak{C}_{ns}^+(67)|) = 16$, we may conclude:

$$\mathcal{C}_{59} \cong (\mathbb{Z}/59\mathbb{Z})^{14} \text{ and } \mathcal{C}_{67} \cong (\mathbb{Z}/67\mathbb{Z})^{14} \times (\mathbb{Z}/67^2\mathbb{Z}).$$

Let q a prime that does not divide $p(p^2 - 1)$. Let $n > 0$ be the order of $q \bmod \frac{p-1}{2}$ and let $\mathfrak{o}_{q,n}$ be the ring of integers in the unramified extension of the q -adic field \mathbb{Q}_q of degree n . We have an analogous decomposition for the q -primary part $\mathcal{C}_{p,q}$ of $\mathfrak{C}_{ns}^+(p)$:

$$R_{p,q} := \mathbb{Z}_q[H] \text{ with } H = (\mathbb{Z}/p\mathbb{Z})^*/(\pm 1),$$

$$R_{p,q,0} := \{x \in R_{p,q} \text{ of degree } 0\},$$

$$\mathcal{C}_{p,q} \cong R_{p,q,0}/R_{p,q}\theta \text{ and } \mathfrak{o}_{q,n} \otimes_{\mathbb{Z}_q} \mathcal{C}_{p,q} = \bigoplus_{\chi} \mathcal{C}_{p,q}(\chi)$$

where χ ranges over the non trivial characters:

$$\chi : (\mathbb{Z}/p\mathbb{Z})^*/(\pm 1) \rightarrow \mathfrak{o}_{q,n}^*.$$

Proposition 3.3. *Let $p \equiv 1 \pmod{4}$ and $q \geq 7$ a prime different from p that does not divide $p^2 - 1$. If q^m is the maximal q -power dividing $|\mathfrak{C}_{ns}^+(p)|$ then m is even.*

Proof. We have $\mathcal{C}_{p,q}(\chi) = \mathfrak{o}_{q,n}/\mathfrak{o}_{q,n}\chi(\theta)$ and from Theorem 4.5 of [6, Chapter 5] if $p \equiv 1 \pmod{4}$ and $\chi_1^2 = \chi_2^2$ we have $\text{ord}_q\chi_1(\theta) = \text{ord}_q\chi_2(\theta)$. If $\chi^2 = 1$ we have $\mathcal{C}_{p,q}(\chi) = 0$. \square

References

- [1] T. Arakawa, T. Ibukiyama, M. Kaneko, *Bernoulli Numbers and Zeta Functions*, Springer Monographs in Mathematics XI, 2014.
- [2] P. Carlucci, *Cuspidal divisor class groups of non-split Cartan modular curves*, arXiv:1605.00375v1.
- [3] H. Cohen, *Number theory. Vol. II. Analytic and modern tools*, Volume 240 of Graduate Texts in Mathematics, Springer, New York, 2007.
- [4] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, 2004.
- [5] D. Kubert and S. Lang, *Cartan-Bernoulli numbers as values of L -functions*, Math. Ann. 240 (1979) pp. 21–26.
- [6] D. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Springer Verlag, New York-Berlin, 1981.
- [7] D. Kubert and S. Lang, *The p -primary component of the cuspidal divisor class group on the modular curve $X(p)$* , Math. Ann. 234 (1978) pp. 25–44.
- [8] S. Lang, *Cyclotomic Fields I and II. Combined second edition with an appendix by Karl Rubin*. Graduate Texts in Mathematics, 121. Springer-Verlag, New York, 1990.
- [9] L.C. Washington, *Introduction to Cyclotomic Fields*, Volume 83 of Graduate Texts in Mathematics, Springer-Verlag, 1982.